HealthManagement
Promoting Management and Leadership

Hackers Could Have Uploaded False Patient Data Via Flawed Mobile App

Two flaws in a mobile medical app that might have permitted fake patient data to be uploaded have been fixed by German software company SAP. Although the issues were addressed before any damage was done, it is a reminder to healthcare organisations about the ongoing threat of security issues which could have devastating medical and legal consequences.

SAP's mobile EMR, Unwired, includes patient data such as lab results and images. One of the discovered flaws could have allowed someone to upload malware or access the database, said Alexander Polyakov, the Chief Technology Officer of ERPScan, which specialises in enterprise application security.

Another flaw could have allowed hackers to "tamper with a configuration file and then change medical records stored on the server," Jeremy Kirk wrote in Computer World.

The latest incidents for SAP highlight the inherent risk that exists in healthcare organisations, no matter the size or sophistication of the company. As technology becomes a tool for greater convenience, companies must proceed with caution and constant vigilance. Fortunately for SAP, the flaws were detected and quickly addressed.

Larger healthcare organisations sometimes see possible breaches as the cost of doing business in the era of digital health. Some may even plan for the potential expenses related to hacking in company budgets. Of course, it is difficult to measure the damage done when consumers and customers lose trust in a brand.

The SAP situation appears on the heels of a high-profile breach at Premera Blue Cross, and not long after Anthem incurred the largest ever data hack, which affected approximately 80 million members.

Source: Computer World

Image Credit: Pixabay

Published on : Tue, 31 Mar 2015